SECRET

DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D.C. 20301

Rec'd 14 MAY 73 DB

24 APR 1973

S-67,239/DS-6C3

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE, UNITED STATES INTELLIGENCE BOARD

SUBJECT: COINS Network Security Enhancements (U)

Reference: DCI Memorandum for the Directors, DIA, NSA, and NPIC, 9 April 1973, subject: COINS.

1. (C) By separate action, this Agency is advising the Executive Agent for COINS, ASD(I), of the readiness of DIA to meet the 1 May target date for the incorporation of SAO material into the DIA component of the COINS network. This expressed DIA readiness extends to currently connected nodes of the IDHSC network (i.e., CONAD and CINCPAC) as well as to the DIA COINS/IDHSC switch and will be accomplished by securing all DIAOLS/IDHSC system components to the TOP SECRET SI/SAO level.

2. (C) The incorporation of SAO material into the COINS network, directed by reference and supported by this Agency, represents a substantial, cost-effective enhancement of network effectiveness to users. With such an expansion of the network information content, both with regard to information volume and subject/source spectrum, together with anticipated network component expansion on the near-term horizon (e.g., IDHSC additions and planned interface between COINS/IDHSC and the NMIC computer network), network security uncertainties and vulnerabilities assume a much greater significance. In view of the foregoing, a comprehensive assessment of and enhancement to the security stature of the COINS/IDHSC network appears mandatory. Appended is a set of recommendations which we feel represent a modest, realistic and cost-effective set of investments in network security responsive to the deficiencies and problems noted below. This material is specifically suggested for incorporation in the Computer Security Subcommittee's response to the memorandum from the Chairman, Security Committee, 10 October 1972, subject: Security Level of COINS (C).

Classified by .....DIADS-6.....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY.....3.....
DECLASSIFY ON CANNOT BE DETERMINED

DIA review completed.

SECRET

3. (S) It is anticipated that the forthcoming COINS subject/source spectrum expansion and information volume growth will significantly increase the value of the COINS/IDHSC network as a hostile intelligence penetration target. Presumably, for example, it was precisely these same qualities that accounted for Soviet interest in penetrating U.S. communications systems, as evidenced by then KGB Chairman Shelepin's 1961 directive to KGB legal residencies to "recruit cipher clerks" as the first priority task. With reference to the COINS/IDHSC network, moreover, it is noted that key pertinent attributes of Soviet intelligence modus operandi include the following: a principal philosophy stressing the achievement of agent penetrations; patience, with a view toward long-term exploitation of recruited assets (e.g., some successful operations enduring for 15 to 20 years or more); and the application of multipronged approaches utilizing agent combinations to achieve information as well as covert action objectives.

4. (C) In the face of the foregoing threat model, it is noted that fundamental and empirical concepts and principles in computer security are only now emerging; moreover, no analogous results in network security are known to exist. The following extracts from the recently completed Air Force Systems Command (ESD) Computer Security Technology Planning Study, in which NSA and DIA representatives participated, allude to the network security problem and its state of the art:

> The security condition of networks is even less structured than that of most (individual shared computer system) applications . . . The security threat posed by such operations is that, in general, the computer to computer communications are accepted as valid on the questionable basis that the other computer has a high security reliability . . . that the security dangers of such interlinking are masked by the apparently "safe" interaction directly between computer systems . . . However, if control of a node can be exercised by a malicious users (sic), the entire network may be compromised. While there are growing requirements for interconnecting computer systems into networks and several networks already exist, the dimensions of the security problem are unknown (emphasis added). More information is needed on both the networks and their security requirements.

5. (C) In general, perceived problems associated with COINS/IDHSC network security include the following: lack of dedicated network security manpower resources; lack of centralized, authoritative network security management and control mechanisms; lack of need-to-know/must-know mechanisms within the network to limit individual access to less than the total network; and as cited above, lack of empirical knowledge in computer network security. With adoption of the appended recommendations, we feel that an acceptable level of risk for the present and future COINS/IDHSC network can be obtained which will permit a greater exploitation of ADP technology in support of intelligence information handling tasks.

FOR THE DIRECTOR:

25X1

1 Enclosure
DIA Security Recommendations
for the COINS/IDHSC Network (C)

DIA Representative
Computer Security Subcommittee

CONFIDENTIAL

DIA Security Recommendations for the COINS/IDHSC Network

1. (C) The following two concurrent actions are recommended for the enhancement of the COINS/IDHSC network security posture:

a. Establishment of an authoritative, centralized network security element composed of resources exclusively dedicated to the task of COINS network security. It is envisioned that this element would form a larger group by periodically meeting with the Information System Security Officers (ISSO's) of the COINS/IDHSC node systems in dealing with computer network security problems. If desired, DIA will arrange for such IDHSC system participation. The basic rationale for this proposal and the following stems from the observation that the present mode of part-time efforts dealing with COINS/IDHSC security problems is not responsive to the magnitude and complexity of the problem in terms of either depth of expertise or timeliness.

b. Sponsorship and funding of a major contract effort involving recognized technical expertise to address the fundamental problems of network security, using the existing network as an experimental tool. If cost emerges as a significant constraint, consideration may be given to joint Intelligence Community sponsorship of such an effort with other elements of the Executive Establishment who envision or plan implementation of computer system networks (e.g., non-intelligence components of the Department of Defense or Department of Justice).

2. (C) Specific functions and tasks to be undertaken collectively by the entities identified in 1.a. and b., above, should include at least the following:

a. Development and implementation of need-to-know/must-know controls for the network;

b. Development of comprehensive, uniform network security requirements, procedures and responsibilities (in effect, a consolidated network security program);

Classified by .....DIADS-6.....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY...3.....
DECLASSIFY ON CANNOT BE DETERMINED

CONFIDENTIAL

c. Together with basic research in network security, review and assess the security stature of the network and develop enhancements for the network security program based upon both surveillance of the network and periodic testing and evaluation of network security controls;

d. Thoroughly analyze and evaluate proposals for terminal/system additions to the network from a security impact point of view.